

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-345819

(43)Date of publication of application : 14.12.2001

(51)Int.Cl.

H04L 12/28

H04Q 7/38

H04L 9/32

(21)Application number : 2000-164519

(71)Applicant : SHARP CORP

(22)Date of filing : 01.06.2000

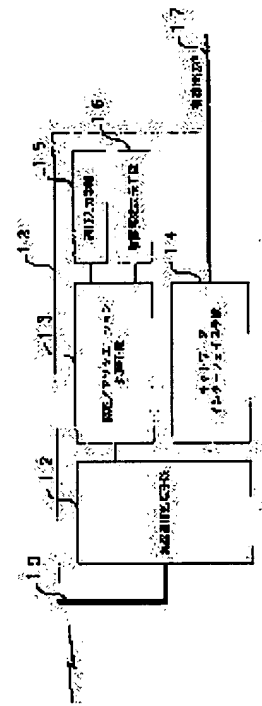
(72)Inventor : KIMURA SHINYA

(54) ACCESS POINT DEVICE AND METHOD OF AUTHENTICATION PROCESSING THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an access point device and a method of authentication processing therefor, with which a security level can be remarkably improved, in a wireless LAN system.

SOLUTION: An access point device 18 is provided with an authentication request display means 16 for making the access point device 18 report the existence of a mobile station requesting authentication for obtaining the final permission of an authentication procedure inside an area, to a network manager for managing a LAN, when the mobile station inside the area is to perform the authentication procedure, before the start of an association procedure and an authentication input means 15 for the network manager, who receives the notice, to instruct the permission of refusal of authentication to the mobile station requesting authentication.



LEGAL STATUS

[Date of request for examination]

19.07.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3585422

[Date of registration] 13.08.2004

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第3585422号
(P3585422)

(45) 発行日 平成16年11月4日 (2004. 11. 4)

(24) 登録日 平成16年8月13日 (2004. 8. 13)

(51) Int. Cl. ⁷

F 1

H 0 4 L 12/28

H 0 4 L 9/32

H 0 4 Q 7/38

H 0 4 L 12/28 3 0 0 Z

H 0 4 B 7/26 1 0 9 R

H 0 4 L 9/00 6 7 3 A

H 0 4 L 9/00 6 7 5 A

請求項の数 6 (全 12 頁)

(21) 出願番号 特願2000-164519 (P2000-164519)
(22) 出願日 平成12年6月1日 (2000. 6. 1)
(65) 公開番号 特開2001-345819 (P2001-345819A)
(43) 公開日 平成13年12月14日 (2001. 12. 14)
審査請求日 平成14年7月19日 (2002. 7. 19)

(73) 特許権者 000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町 2 2 番 2 2 号
(74) 代理人 100091096
弁理士 平木 祐輔
(72) 発明者 木村 真也
大阪府大阪市阿倍野区長池町 2 2 番 2 2 号
シャープ株式会社内

審査官 石井 研一

最終頁に続く

(54) 【発明の名称】 アクセスポイント装置及びその認証処理方法

(57) 【特許請求の範囲】

【請求項 1】 有線伝送路で構築されるネットワークとの
インターフェース機能を備え、無線 LAN エリア内で複
数の移動局とデータリンク接続を行うアクセスポイント
装置において、
複数の移動局とのデータリンク確立を行うためのアソシ
エーション手順と認証手順を実行する認証／アソシエ
ーション実行手段と、
前記エリア内の移動局が、前記アソシエーション手順を
開始する前に前記認証手順を行おうとする場合に、前記
LAN を管理するネットワーク管理者に対し、認証手順
の最終的な許可を得るために、認証を求めている移動局
がいることを通知する通知手段と、
前記通知を受けた前記ネットワーク管理者による、前記
認証を求めている移動局に対しての認証の許可又は拒否

の指示が入力される入力手段と、

を備えることを特徴とするアクセスポイント装置。

【請求項 2】 前記通知手段は、前記ネットワーク管理者
に対して、前記認証手順の最終的な許可を通知するとと
もに、最終認証が行われるまでの最大待ち時間を設定し
た認証待ちタイマをスタートし、
前記認証待ちタイマがタイムアウトする前に、前記ネッ
トワーク管理者による、前記認証を求めている前記移動
局に対しての認証の許可の指示が入力されたとき、認証
応答メッセージを、認証許可として前記移動局に返信す
ることを特徴とする請求項 1 記載のアクセスポイント装
置。

【請求項 3】 有線伝送路で構築されるネットワークとの
インターフェース機能を備え、無線 LAN エリア内で複
数の移動局とデータリンク接続を行うアクセスポイント

3

装置の認証処理方法において、
前記移動局から前記アクセスポイント装置への認証要求により、前記移動局及び前記アクセスポイント装置が、所定の認証手続を開始する第1ステップと、
前記認証手続により、前記アクセスポイント装置が、前記移動局への認証を許可しようとするとき、前記認証手続における最終メッセージである認証応答メッセージを前記移動局に返信する前に、前記LANを管理するネットワーク管理者に対して、前記認証手順の最終的な許可を通知するとともに、最終認証が行われるまでの最大待ち時間を設定した認証待ちタイマをスタートさせる第2ステップと、
前記ネットワーク管理者が、前記アクセスポイント装置に対して、前記認証待ちタイマがタイムアウトする前に、最終の認証の許可又は拒否を指示する第3ステップと、
前記ネットワーク管理者により、前記認証待ちタイマがタイムアウトする前に、最終の認証許可が指示されると、前記アクセスポイント装置が、前記認証応答メッセージを、認証許可として前記移動局に返信する第4ステップと、
前記認証応答メッセージを受信した前記移動局が、アソシエーションの手順を開始する第5ステップと、
を実行することにより前記移動局の認証が完了し、アソシエーション手順を開始することを特徴とするアクセスポイント装置の認証処理方法。

【請求項4】前記第3ステップでは、前記ネットワーク管理者が、認証を拒否する指示を前記アクセスポイント装置に指示した場合に、前記認証応答メッセージを、認証拒否として前記移動局に返信することを特徴とする請求項3記載のアクセスポイント装置の認証処理方法。

【請求項5】前記第3ステップでは、前記ネットワーク管理者が、認証を拒否又は許可する指示を前記アクセスポイント装置に指示する前に、前記認証待ちタイマがタイムアウトすると、前記認証応答メッセージを、認証拒否として前記移動局に返信することを特徴とする請求項3記載のアクセスポイント装置の認証処理方法。

【請求項6】前記認証手続は、IEEE802.11が規定するShared Key Authentication手順であることを特徴とする請求項3乃至5のいずれかに記載のアクセスポイント装置の認証処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、アクセスポイント装置及びその認証処理方法に関し、詳細には、無線を利用した、ワイヤレスLANシステムにおいて、悪意を持った侵入者の移動局からの

4

不正なアクセスを防止するためのアクセスポイント装置及びその認証処理方法に関する。

【0002】

【従来の技術】

近年、インターネットの爆発的な普及に伴い、オフィス、家庭等で、LAN(Local Area Network)を構築するケースが増えてきている。デジタル無線通信技術の進歩も手伝い、ケーブル配線の煩わしさから、無線でLANを構築する、いわゆるワイヤレスLANのニーズも非常に高まっており、さらに、ノート型パソコンに代表される移動端末での移動環境下における、使用が可能であることも手伝い、将来的には、かなりの数の普及台数が期待されている。このワイヤレスLANの代表的な技術としては、既に、IEEE(Institute of Electrical and Electronics Engineers)において、標準化されている、IEEE802.11がある。この標準化された技術は、OSIモデルにおける、物理層から、データリンクの下位副層であるMAC(Media Access Control:媒体アクセス制御)層までを規定しており、有線のLAN伝送路である、イーサネットと置きかえることができ、さらに、ワイヤレスであるが故の付加機能として、ローミング(roaming)機能も提供できる仕様になっている。

【0003】

さて、有線のイーサネット等で、LANを構築する場合、LANに接続することは、物理的に、ハブ等にケーブルを接続するため、データリンクレベルのセキュリティレベルは非常に高い。つまり、侵入者が、オフィス等に不正に侵入し、端末等をネットワークに接続しようと思っても、ケーブル接続という物理的な作業が必要であり、それを、密に行うことは、一般的なLANの配置状況(特に、比較的中小規模のLAN)からして、非常に困難である。何故なら、そのLANの利用者と、そのLANを構成するハブやルーター等が、同一の居室内に存在するケースが殆どだからである。一方、ワイヤレスLANシステムの場合は、前記、イーサネット等のケーブル接続の作業は、自動的なアソシエーション(association)手順により置き換わる。前記、既存のIEEE802.11等のシステムにおいて、このアソシエーション手順とは、移動端末が有線等のバックボーン・ネットワークに接続されているアクセスポイントに対して、自分自身の存在を認識してもらうための手順であり、この手順が完了すれば、データ通信を行うことができる。この手順においては、アクセスポイント(access point)のカバーする有限エリアにいる移動端末は、前記アクセスポイントに対して、アソシエーションを行う前に、オプションの認証手続きをするにより、データリンクレベルのセキュリティを

確保することになる。

【0004】

このアソシエーション手順によれば、前記移動局は、アソシエーション要求を、前記アクセスポイントに対して行う場合、そのアソシエーション要求メッセージ中に、SSID (Service Set Identifier) を含ませ、これを受信したアクセスポイントは、前記SSIDにて、前記移動局を識別し、予め決められたアソシエーション許可ルールに従い、そのアソシエーションを許可するかどうかを決定し、許可する場合は、アソシエーション許可の返信メッセージを、拒否する場合は、アソシエーション拒否の返信メッセージを、前記移動局に送信する。したがって、このアソシエーション手順だけでは、悪意を持ってネットワークに侵入しようとする者が、このSSIDさえ入手してしまえば、簡単にアソシエーションが可能になってしまう。それを避けて、本アソシエーション手順を実行するために、認証手続きを行うオプションが設けられている。つまり、認証手続きを行うオプションを設ける方式によれば、前記移動端末は、本認証手続きを完了しなければ、アソシエーションができないため、データ通信を開始することができず、これは、物理的な接続作業を必要としない、前記有限エリア内の、悪意を持った移動端末からの、不正なアソシエーションを防ぐ有効な機能を提供することになる。

【0005】

IEEE802.11においては、この認証手続きは、Shared Key Authentication 手順として定義されており、この手順を図5及び図6により説明する。図5は、従来のワイヤレスLANシステムの概略構成を示す図、図6は、従来の認証手順とアソシエーション手順の制御シーケンスを示す図である。

【0006】

図5において、1はワイヤレス・エリア・ネットワーク、2はアクセスポイントAP、3は移動局MT1、4は移動局MT2、5は移動局MT3、6は移動局MT4、7はワイヤレス・エリア・ネットワーク1外他ネットワークである。

【0007】

ある有線伝送路により実現される、他ネットワーク7に接続されたアクセスポイントAP2と、そのアクセスポイントAP2がカバーする、有限なエリアに存在する、移動局MT1、MT2、MT3、MT4から構成されるワイヤレス・エリア・ネットワーク1において、ある移動局(例えば、MT1)が、電源を投入するなどの動作により、前記アクセスポイントAP2に対して、アソシエーション前の認証手続きをする場合のシーケンスは、図6に示される。

【0008】

まず、移動局MT1は、Shared Key Authentication 方法による認証手続きを開始するための、認証要求メッセージ1を、アクセスポイントAP2に送信する。AP認証処理8 (AP認証処理「1」)として、このメッセージを受信したAP2は、この認証手続きの度に、任意に決めることができる、Initialization VectorとSecret Keyの値を、パラメータとし、WEP (Wired Equivalent Privacy) PRNG (Pseudorandom Number Generator) のアルゴリズムに従い数値演算を行い、128Octetの、一意に決まるChallenge Textの値を算出し、この値を含めた認証応答メッセージ1を、移動局MT1に送信する。

【0009】

次に、MT認証処理9 (AP認証処理「2」)として、本認証応答メッセージ1を受信した移動局MT1は、その中含まれる前記Challenge Textの値を、WEPの暗号化アルゴリズムに従い、Shared Secret Dataと、Initialization Vectorをパラメータに、暗号化を行い、その値を、前記Initialization Vectorと共に、認証要求メッセージ2に含めて、前記アクセスポイントAP2に返信する。

【0010】

さらに、AP認証処理10 (AP認証処理「2」)として、本認証要求メッセージ2を受信した、アクセスポイントAP2は、受信した暗号化されたChallenge Textの値を、同時に受信したInitialization Vectorと、予め知っている前記Shared Secret Dataを基にデコードし、その結果と、前述の元のChallenge Textの値を比較し、それが同一であれば、認証許可とし、同一でなければ、認証拒否とし、その結果を認証応答メッセージ2として、移動局MT1に返信する。そこで、本認証応答メッセージ2を受信した移動局MT1は、その結果が、許可であれば、次のアソシエーションの手順に入ることができ、拒否の場合は、認証失敗ということで、アソシエーション手続きを行うことはできない。

【0011】

ここでのアソシエーション処理は、前述の通り、移動局MT1からの、アソシエーション要求メッセージ中の、SSID (Service Set Identifier) を受信したアクセスポイントAP2が、前記SSIDにて、移動局を識別し、予め決められたアソシエーション許可ルールに従い、そのアソシエーションを許可するかどうかを決定し、許可する場合は、アソシエーション許可のアソシエーション応答メッセージを、拒否する場合は、アソシエーション拒否のアソシエーション応

答メッセージを移動局MT1に送信する。なお、ここのWE Pのアルゴリズムは、RSA Data Security Inc. のRC4技術により規定されている。

【0012】

つまり、この認証方法によれば、アクセスポイントと移動局が、あらかじめ、秘密のKeyであるShared Secret Keyを持ち合うことで、アクセスポイントが特定の移動局への認証／アソシエーションを許可する仕組みを実現している。ここで、移動局側は、本Shared Secret Keyを、一般ユーザから、読み取れない実装形態にし、悪意を持った侵入者からの盗難（読み取り）を防ぎ、本Key自体が無線伝送路を行き交うことがないので、傍受されることもなく、ある程度のセキュリティレベルを確保している。

【0013】

【発明が解決しようとする課題】

しかしながら、このような従来のアクセスポイント装置の認証処理方法にあつては、認証のためのアルゴリズムと、その認証のためのKeyが、悪意を持ってネットワークに侵入しようとする者に、不正に盗まれないという前提でのセキュリティの確保であり、この前提は100%担保できるものではない。すなわち、正式手順によってアクセスポイントに、認証可能な端末の全くのコピーが、作られないという保証はなく、また、そのユーザからアクセスできないメモリに、格納されているKeyが、特殊な機器を使うことで、不正に読み取られる可能性もないとはいいきれない。よって、これらの不正な行為によって、悪意を持ってネットワークに、侵入しようとする者が、ある端末を不正にアソシエーションすることができれば、有線のケーブル接続のような物理的な作業なしに、アクセスポイントのカバーするエリアであれば、物理的に、隠れてネットワークに侵入することができる。つまり、ある閉じられた空間（オフィスや、家庭）内で、ワイヤレスネットワークを構築した場合で、その中心にあるアクセスポイントのカバーするエリア内であれば、その閉じられた区間の外部、つまり、壁等で隔てられた死角にある、悪意を持ってネットワークに侵入しようとする者の端末からのアソシエーションを許してしまう可能性があるという問題があった。

【0014】

本発明は、このような課題に鑑みてなされたものであつて、ワイヤレスLANシステムにおいて、セキュリティレベルを飛躍的に向上させることができるアクセスポイント装置及びその認証処理方法を提供する。

【0015】

【課題を解決するための手段】

本発明のアクセスポイント装置は、有線伝送路で構築されるネットワークとのインターフェース機能を備え、無線LANエリア内で複数の移動局とデータリンク接続を

行うアクセスポイント装置において、複数の移動局とのデータリンク確立を行うためのアソシエーション手順と認証手順を実行する認証／アソシエーション実行手段と、前記エリア内の移動局が、前記アソシエーション手順を開始する前に前記認証手順を行おうとする場合に、前記LANを管理するネットワーク管理者に対し、認証手順の最終的な許可を得るために、認証を求めている移動局がいることを通知する通知手段と、前記通知を受けた前記ネットワーク管理者による、前記認証を求めている移動局に対しての認証の許可又は拒否の指示が入力される入力手段と、を備えることを特徴とする。

【0016】

本発明のアクセスポイント装置の認証処理方法は、有線伝送路で構築されるネットワークとのインターフェース機能を備え、無線LANエリア内で複数の移動局とデータリンク接続を行うアクセスポイント装置の認証処理方法において、前記移動局から前記アクセスポイント装置への認証要求により、前記移動局及び前記アクセスポイント装置が、所定の認証手続を開始する第1ステップと、前記認証手続により、前記アクセスポイント装置が、前記移動局への認証を許可しようとするとき、前記認証手続における最終メッセージである認証応答メッセージを前記移動局に返信する前に、前記LANを管理するネットワーク管理者に対して、前記認証手順の最終的な許可を通知するとともに、最終認証が行われるまでの最大待ち時間を設定した認証待ちタイマをスタートさせる第2ステップと、前記ネットワーク管理者が、前記アクセスポイント装置に対して、前記認証待ちタイマがタイムアウトする前に、最終の認証の許可又は拒否を指示する第3ステップと、前記ネットワーク管理者により、前記認証待ちタイマがタイムアウトする前に、最終の認証許可が指示されると、前記アクセスポイント装置が、前記認証応答メッセージを、認証許可として前記移動局に返信する第4ステップと、前記認証応答メッセージを受信した前記移動局が、アソシエーションの手順を開始する第5ステップと、を実行することにより前記移動局の認証が完了し、アソシエーション手順を開始することを特徴とする。

【0017】

また、前記第3ステップでは、前記ネットワーク管理者が、認証を拒否する指示を前記アクセスポイント装置に指示した場合に、前記認証手続における最終メッセージである認証応答メッセージを、認証拒否として前記移動局に返信するものであつてもよい。

【0018】

また、前記第3ステップでは、前記ネットワーク管理者が、認証を拒否又は許可する指示を前記アクセスポイント装置に指示する前に、前記認証待ちタイマがタイムアウトすると、前記認証手続における最終メッセージである認証応答メッセージを、認証拒否として前記移動局に

返信するものであってもよい。

また、好ましい具体的な態様としては、前記認証手続は、IEEE802.11が規定するShared Key Authentication手順であっててもよい。

【0019】

【発明の実施の形態】

以下、添付図面を参照しながら本発明の好適なアクセスポイント装置及びその認証処理方法の実施の形態について詳細に説明する。

図1は、本発明の実施の形態のアクセスポイント装置の概略構成を示す図である。

【0020】

本実施の形態のアクセスポイント装置18は、前記図5のアクセスポイントAP2に置き換えて設置される。すなわち、前記図5において、ある有線伝送路により実現される、他ネットワーク7に接続された、アクセスポイントAP2と、そのAP2がカバーする、有限なエリアに存在する移動局MT1、MT2、MT3、MT4から構成される、ワイヤレス・エリア・ネットワーク1において、前記アクセスポイントAP2は、図1に示すアクセスポイント装置18に置き換えて構成される。

【0021】

図1において、アクセスポイント装置18は、複数の移動局MT1、MT2、MT3、MT4との無線接続を実現するために、無線変復調部、ベースバンド信号処理部及びデータリンク制御部からなる無線通信処理手段12と、無線通信処理手段12に接続される無線送受信用のアンテナ19と、他ネットワーク7と任意の有線伝送路17によりデータリンク接続し、無線通信処理手段12により送受信されるデータをインターフェースする機能を実現するネットワークインターフェース手段14と、無線通信処理手段12が、複数の移動局とのデータリンク確立を行うためのアソシエーション手順と認証手順を実行し、そこで、必要になる、移動局MT1、MT2、MT3、MT4と交換される制御メッセージを無線通信処理手段12とやりとりする機能を実現する認証／アソシエーション処理手段13と、認証／アソシエーション処理手段13が、認証処理を行う場合に、最終的にそれを許可し、認証許可すべき移動局に認証許可のメッセージを送信する前に、それを通知することで、ワイヤレス・エリア・ネットワーク1を管理するユーザに、表示デバイスやスピーカ等で認証要求している移動局の存在を通知する機能を実現する認証要求表示手段16（通知手段）と、認証要求表示手段16により認証要求している移動局の存在が通知された後に、ワイヤレス・エリア・ネットワーク1を管理するユーザが、それを許可又は拒否することを、認証／アソシエーション処理手段13に通知するためにボタン等の人間の物理的な入力を受け付ける機能を実現する認証入力手段15（入力手段）とか

ら構成される。

【0022】

以下、上述のように構成されたアクセスポイント装置の認証処理方法の動作を説明する。

ここでは、ある移動局が、電源投入等の動作により、認証処理手順とアソシエーション処理手順が実行され、アクセスポイント装置18とのデータリンク接続が確立される場合と認証が拒否される場合のシーケンスを説明する。

10 【0023】

前記図5における移動局MT1を、認証処理を行う対象の移動局とし、移動局MT2、MT3、MT4は、既にアクセスポイント装置18とアソシエーションまで完了し、データリンクが確立しているものとする。

まず、移動局MT1が、認証手続きにより、ネットワークを管理するユーザが、その認証を許可し、その後、アソシエーション手続きにより、アクセスポイント装置18とのデータリンクが確立される場合を、図2及び図4を参照して説明する。

20 【0024】

図2は、認証許可の場合の認証手順の制御シーケンスを示す図である。

移動局MT1が、電源投入等の動作により、まず、Shared Key Authentication方法による認証手続きを開始するための認証要求メッセージ1をアクセスポイント装置18に送信する。

【0025】

アクセスポイント装置18において、無線通信処理手段12を介して、このメッセージを受信した認証／アソシエーション処理手段13は、AP認証処理1（図2の番号20参照）として、この認証手続きの度に、任意に決めることができる、Initialization VectorとSecret Keyの値をパラメータとし、WEP（Wired Equivalent Privacy）PRNG（Pseudorandom Number Generator）のアルゴリズムに従い数値演算を行い、128Octetの一意に決まるChallenge Textの値を算出し、この値を含めた認証応答メッセージ1を無線通信処理手段12を介して移動局MT1に送信する。

40 【0026】

次に、MT認証処理21として、本認証応答メッセージ1を受信した、移動局MT1は、その中に含まれるChallenge Textの値を、WEPの暗号化アルゴリズムに従い、Shared Secret DataとInitialization Vectorをパラメータにして暗号化を行い、その値をInitialization Vectorと共に、認証要求メッセージ2に含めてアクセスポイント装置18に返信する。さらに、アクセスポイント装置18において、無線通信

11

処理手段12を介して、このメッセージを受信した認証／アソシエーション処理手段13は、AP認証処理2

(図2の番号22参照)として、受信した暗号化されたChallenge Textの値を、同時に受信したInitialization Vectorと予め知っているShared Secret Dataを基にデコードし、その結果と前述の元のChallenge

Textの値を比較し、それが同一であれば、AP認証処理3(図2の番号23参照)の手順を実行する。この手順を示したのが図4に示すフローのステップS30

～ステップS33の処理である。

【0027】
図4は、上記アクセスポイントの認証処理を示すフローチャートである。

まず、この手順においては、アクセスポイント装置18の認証／アソシエーション処理手順13は、認証要求表示手段16に対して、認証待ちであることを通知し(ステップS30)、それと同時に、任意の時間に設定された認証待ちタイマをスタートさせ(ステップS31)、認証入力待ち(ステップS32)の状態に入る。一方、認証待ちであることの通知を受けた、認証要求表示手段16は、直ぐに、ネットワークを管理するユーザに対して表示デバイスやスピーカ等で認証要求している移動局が存在することを通知する。

【0028】

ここで、認証／アソシエーション処理手順13は、認証待ちタイマがタイムアウトする前に認証入力手段16からのネットワークを管理するユーザの認証許可の入力による認証許可入力の通知を受ければ、認証許可を示した認証応答メッセージ2を無線通信処理手段12を介して移動局MT1に送信する(ステップS33)。

【0029】

図2に戻って、本認証応答メッセージ2を受信した移動局MT1は、その結果が、許可であることから、次のアソシエーションの手順に入り、アソシエーション要求メッセージを、アクセスポイント装置18へ送信する。

【0030】

ここで、アクセスポイント装置18においては、無線通信処理手段12を介して、このメッセージを受信した認証／アソシエーション処理手段13は、アソシエーション処理(図2の番号24参照)として、アソシエーション要求メッセージ中のSSID(Service Set Identifier)にて、移動局MT1を識別し、予め決められたアソシエーション許可ルールに従い、そのアソシエーションを許可するかどうかを決定し、それを許可するときは、無線通信処理手段12を介して移動局MT1へアソシエーション許可を示したアソシエーション応答メッセージを送信する。このアソシエーション応答メッセージを移動局MT1が受信すれば、移動局MT1とアクセスポイント装置18の間でデータ

12

リンクが確立され、以降、データの通信が可能になる。

【0031】

次に、移動局MT1が、認証手続きにおいて、ネットワークを管理するユーザにより、その認証を拒否される場合、及び、認証待ちタイマがタイムアウトして、自動的に、認証が拒否される場合を図3及び図4を参照して説明する。

【0032】

図3は、認証拒否／タイムアウト場合の認証手順の制御シーケンスを示す図である。

図3において、移動局MT1が、電源投入等の動作により、Shared Key Authentication方法による認証手続きを開始するための認証要求メッセージ1をアクセスポイント装置18に送信する。

【0033】

アクセスポイント装置18において、無線通信処理手段12を介して、このメッセージを受信した認証／アソシエーション処理手段13は、AP認証処理1(図3の番号25参照)としてこの認証手続きの度に、任意に決めることができる、Initialization VectorとSecret Keyの値をパラメータとし、WEP(Wired Equivalent Privacy)PRNG(Pseudorandom Number Generator)のアルゴリズムに従い数値演算を行い、1280ctetの一意に決まるChallenge Textの値を算出し、この値を含めた認証応答メッセージ1を、無線通信処理手段12を介して、移動局MT1に送信する。

【0034】

次に、MT認証処理(図3の番号26参照)として、本認証応答メッセージ1を受信した移動局MT1は、その中含まれるChallenge Textの値を、WEPの暗号化アルゴリズムに従い、Shared Secret Dataと、Initialization Vectorをパラメータに暗号化を行い、その値をInitialization Vectorと共に、認証要求メッセージ2に含めてアクセスポイント装置18に返信する。さらに、アクセスポイント装置18において、無線通信処理手段12を介して、このメッセージを受信した認証／アソシエーション処理手段13は、AP認証処理2(図3の番号27参照)として受信した暗号化されたChallenge Textの値を、同時に受信したInitialization Vectorと予め知っているShared Secret Dataを基にデコードし、その結果と前述の元のChallenge Textの値を比較し、それが同一であればAP認証処理3(図3の番号28参照)の手順を実行する。この手順を示したのが図4に示すフローのステップS30～ステップS32、ステップS34の処理である。

【0035】

まず、この手順においては、アクセスポイント装置18の認証／アソシエーション処理手順13は、認証要求表示手段16に対して認証待ちであることを通知し（ステップS30）、それと同時に、任意の時間に設定された認証待ちタイマをスタートさせ（ステップS31）、認証入力待ち（ステップS32）の状態に入る。一方、認証待ちであることの通知を受けた認証要求表示手段16は、直ぐに、ネットワークを管理するユーザに対して表示デバイスやスピーカ等で認証要求している移動局が存在することを通知する。

【0036】

ここで、認証／アソシエーション処理手順13は、認証待ちタイマがタイムアウトする前に認証入力手段16からのネットワークを管理するユーザの認証拒否の入力による認証拒否入力の通知を受ければ、認証拒否を示した認証応答メッセージ2を無線通信処理手段12を介して移動局MT1に送信する（ステップS34）。同様に、認証入力待ち（ステップS32）の状態において、認証待ちタイマがタイムアウトすれば、認証拒否を示した認証応答メッセージ2を無線通信処理手段12を介して移動局MT1に送信する（ステップS34）。

【0037】

図3に戻って、本認証応答メッセージ2を受信した移動局MT1は、その結果が拒否であることから次のアソシエーションの手順には入れず、必要があれば、ユーザに対して認証が失敗したことを通知する（図3の番号29参照）。よって、この場合は、移動局MT1は、データ通信を行うことができない。

【0038】

なお、ここで言及している、WEPのアルゴリズムは、RSA Data Security Inc.のRC4技術により規定されており、また、アソシエーション処理（図2の番号24参照）も、IEEE802.11で規定されるアソシエーション手順と同一であることとする。

【0039】

また、ここでの認証待ちタイマに設定されている任意の時間とは、ネットワークを管理するユーザが、認証要求表示手段により、認証待ちの移動局が存在することを認識してから、それを許可するために、認証入力手段により、許可の入力をするまでに必要な時間から換算される妥当な値として、ネットワークを管理するユーザが、任意に設定可能であるものとする。

【0040】

以上述べたように、本実施の形態では、アクセスポイント装置18は、エリア内の移動局が、アソシエーション手順を開始する前に認証手順を行う場合に、アクセスポイント装置18が、LANを管理するネットワーク管理者に対し、認証手順の最終的な許可を得るために、認証

を求めている移動局がエリア内にいることを通知する認証要求表示手段16と、通知を受けたネットワーク管理者が、認証を求めている移動局に対して認証の許可又は拒否を指示する認証入力手段15とを備え、物理的に目視できないがために、悪意を持った、ネットワークへの侵入者の攻撃を受けやすい、ワイヤレスLANシステムにおいて、移動局のアソシエーション前の認証手続きで、アクセスポイントがそれを許可することを自動的に行わず、そのネットワークを管理するユーザが、誰がアソシエーションしようとしているのかを目視した上で、その許可を与えることができるので、セキュリティレベルを飛躍的に向上させることができる。

【0041】

また、この認証の手順は、IEEE802.11で、オプションとして規定されている、Shared Key Authentication手順を実装しているワイヤレスLANシステムにおいては、アクセスポイント装置についてのみ追加の実装が必要であり、移動局装置は、なんら変更をすることなく機能させることが可能である。

【0042】

【発明の効果】

以上、詳述したように、本発明によれば、ワイヤレスLANシステムにおいて、セキュリティレベルを飛躍的に向上させることができ、また、移動局装置は、なんら変更をすることなく実施することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態のアクセスポイント装置の概略構成を示す図である。

【図2】本実施の形態のアクセスポイント装置の認証許可の場合の認証手順の制御シーケンスを示す図である。

【図3】本実施の形態のアクセスポイント装置の認証拒否／タイムアウト場合の認証手順の制御シーケンスを示す図である。

【図4】本実施の形態のアクセスポイント装置のアクセスポイントの認証処理を示すフローチャートである。

【図5】従来のワイヤレスLANシステムの概略構成を示す図である。

【図6】従来のワイヤレスLANシステムの認証手順とアソシエーション手順の制御シーケンスを示す図である。

【符号の説明】

- 1 ワイヤレス・エリア・ネットワーク
- 3 移動局MT1
- 4 移動局MT2
- 5 移動局MT3
- 6 移動局MT4
- 7 他ネットワーク
- 12 無線通信処理手段
- 13 認証／アソシエーション処理手段

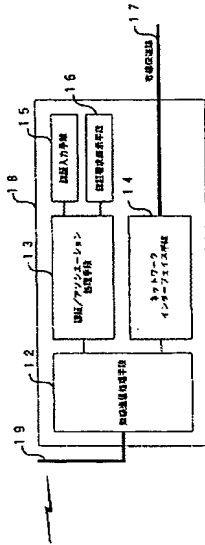
15

- 14 ネットワークインターフェース手段
 15 認証入力手段（入力手段）
 16 認証要求表示手段（通知手段）

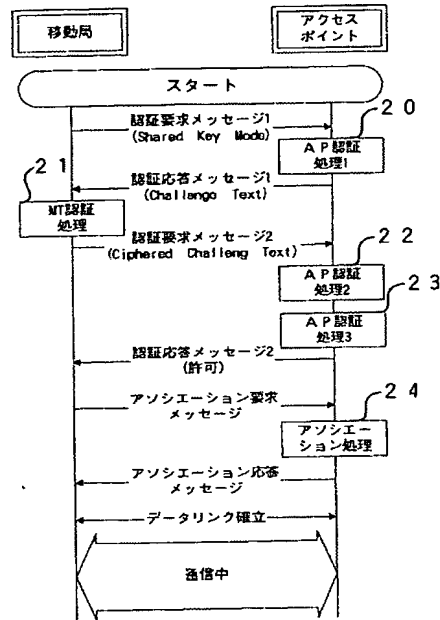
16

- 17 有線伝送路
 18 アクセスポイント装置
 19 無線送受信用のアンテナ

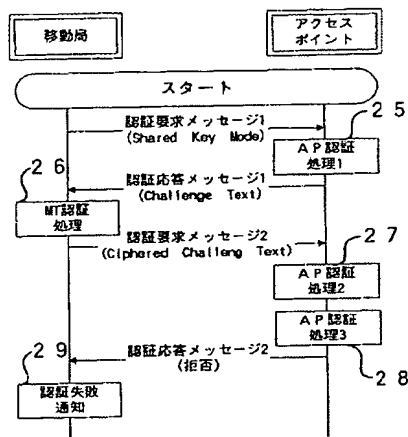
【図1】



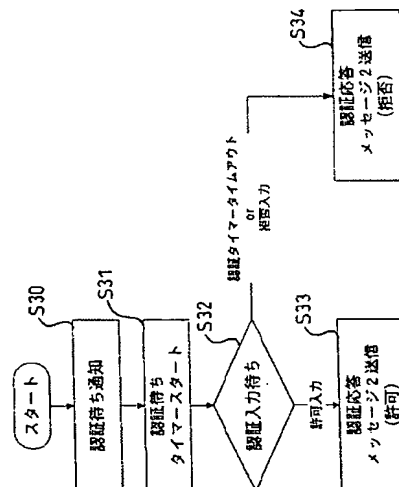
【図2】



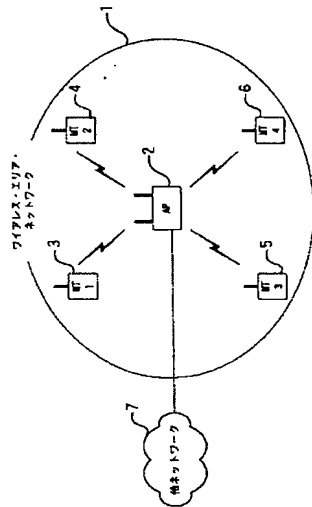
【図3】



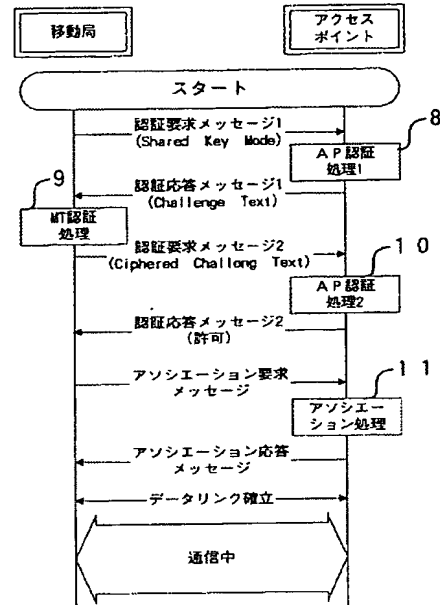
【図4】



【図5】



【図6】



フロントページの続き

(56) 参考文献 特開平10-070540 (JP, A)

特開2000-003336 (JP, A)

A. R. Prasad et al., Security architecture for wireless LANs: corporate & public environment, Vehicular Technology Conference Proceedings, 2000. VTC 2000-Spring Tokyo. 2000 IEEE 51st, 2000年 5月18日, Vol. 1, pp. 283-287

(58) 調査した分野(Int. Cl.⁷, DB名)

H04L 12/28 300

H04L 9/32

H04Q 7/38